SENATE JUDICIARY SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

Hearing on Computer Viruses

May 15, 1989
10:00 a.m., SD-226

WITNESSES

Panel I

William Sessions, Director, Federal Bureau of Investigations

William A. Bayse, Assistant Director of Technical Services Division, FBI

Kenneth Walton, Deputy Assistant Director of Criminal Investigative Division, FBI

Panel II

Clifford Stoll, Computer Astronomer at Harvard-Smithsonian Center for Astrophysics

U.S. SENATOR PATRICK LEAHY

VERMONT

OPENING STATEMENT
BY SENATOR PATRICK LEAHY
Hearing on Computer Viruses
May 15, 1989

Good morning. I am very pleased to welcome our witnesses: Director Sessions, his FBI experts on computer crime investigation, Mr. Walton and Mr. Bayse, and Mr. Stoll, a Space Scientist at the Harvard-Smithsonian Center for Astrophysics. Mr. Stoll is best known for tracking down the West German spy who used computer networks to get into the computers at the Lawrence Berkeley Laboratory. I am delighted to have all of you with us.

As we move into the hi-tech age, we become increasingly reliant on computers for research, communications, and data storage and retrieval. Research is collaborative -- just look at how discoveries were made in superconductivity. As a nation, we cannot afford data that scientists cannot trust. We cannot afford to have scientists refusing to use computer networks to share their discoveries, and thus, advance technology.

Press accounts have focused attention on the alarming number of new techniques -- computer viruses, worms and Trojan horses -- that can secretly enter computers. Their names belie their insidious nature. Hidden programs can destroy or alter data, or, as we saw with the November INTERNET worm, they can hopelessly clog computer networks.

Some of these incidents are malicious. And make no mistake, we will bring the full force of the law to bear on those cases.

Other incidents may reveal genius and creativity rather than malice. These cases pose different, and, in some ways, more difficult policy questions for Congress, for schools and universities, for law enforcement and for American businesses using computers.

The sophistication and ease some American kids demonstrate using computers never cease to amaze me. We cannot unduly inhibit that inquisitive thirteen-year-old who, if left to experiment today, may, tomorrow, develop the telecommunications or computer technology to lead the United States into the 21st century. He represents our future and our best hope to remain a technologically competitive nation.

But, trespassing, breaking and entering, and stealing are against the law. They have always been against the law because they are contrary to the values and principles that society holds dear. That has not and will not change.

Today I am glad to say that hackers are on notice that basic American principles -- principles about respect for the property and privacy of others -- apply to young geniuses, just as they apply to the rest of us.

Just as a kid who enters another's property is trespassing,

or who goes into another's home is breaking and entering,

or who takes another's apple is stealing,

so, too, a hacker who manipulates or destroys the computer program of another -- or who renders it inoperable -- is breaking the law. As a society, we cannot tolerate that.

Director Sessions points out that the FBI will not tolerate it, either. The Bureau treats the creators of disruptive viruses the same way it treats other criminals. I want to be sure the Bureau has the resources to continue to fight this plague on our nation's computer networks.

To do that, we in Congress must start with an understanding of the threat posed by viruses, worms and other potentially destructive programs. And we must do all we can to promote a culture of compliance among computer professionals and to encourage creativity within the context of ethical norms, for all computer users.

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

OPENING STATEMENT

OF

WILLIAM S. SESSIONS

DIRECTOR

FEDERAL BUREAU OF INVESTIGATION

BEFORE AN

OPEN SESSION OF THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

COMMITTEE ON THE JUDICIARY

UNITED STATE SENATE

WASHINGTON, D.C.

MAY 15, 1989

THANK YOU, MR. CHAIRMAN, FOR THE OPPORTUNITY TO BE HERE TODAY TO PRESENT THE FBI'S VIEWS ON THE ISSUE OF COMPUTER VIRUSES. ACCOMPANYING ME THIS MORNING ARE TWO OTHER REPRESENTATIVES FROM THE FBI, WHOSE TECHNICAL EXPERTISE CAN GREATLY ASSIST THIS COMMITTEE. THEY ARE THE ASSISTANT DIRECTOR OF OUR TECHNICAL SERVICES DIVISION, AL BAYSE, WHO IS EXTREMELY KNOWLEDGEABLE ABOUT COMPUTERS AND VIRUSES, AND DEPUTY ASSISTANT DIRECTOR KEN WALTON, OF OUR CRIMINAL INVESTIGATIVE DIVISION. MR. WALTON CAN DETAIL OUR INVESTIGATIVE EXPERIENCES WITH VIRUSES AND OTHER COMPUTER CRIMES. MY PURPOSE IN BEING HERE TODAY IS TO INDICATE TO THIS COMMITTEE THE POTENTIAL SERIOUSNESS OF COMPUTER VIRUSES AND TO ASSURE THE AMERICAN PEOPLE THAT THE FBI IS ACTIVELY INVOLVED IN THE INVESTIGATION OF COMPUTER-RELATED CRIMINAL ACTIVITY.

THE COMMITTEE REQUESTED THAT WE PROVIDE COMMENTS ON THE FBI'S EXPERIENCE IN THE INVESTIGATION OF COMPUTER VIRUSES AND OTHER COMPUTER CRIME. BEFORE I ADDRESS THIS QUESTION, LET ME PUT THE ISSUE OF COMPUTER-RELATED CRIME IN PERSPECTIVE. NOT LONG AGO, COMPUTER EQUIPMENT AND

PROGRAMMING LANGUAGE WERE SO FOREIGN TO THE AVERAGE PERSON THAT THEN-EXISTING COMPUTER SECURITY WAS LARGELY ADEQUATE TO ADDRESS THE EXISTING THREAT. NETWORKS, BULLETIN BOARDS, AND INSTANTANEOUS GLOBAL COMMUNICATIONS AMONG MULTIPLE COMPUTER USERS WERE MUCH LESS COMMON THAN THEY ARE TODAY.

THE EVOLUTION OF TECHNOLOGY, HOWEVER, HAS MADE COMPUTER LITERACY AND ACCESSIBILITY COMMONPLACE. THIS HAS GIVEN OPPORTUNITIES FOR COMPUTER-RELATED CRIMINAL ACTIVITY TO ALMOST EVERYONE, FROM EXPERIENCED CRIMINALS TO TEENAGE "HACKERS." THE MASS MARKETING OF PERSONAL COMPUTERS, THE SIMPLIFICATION OF PROGRAMMING, AND THE ACCESSIBILITY OF PRE-PACKAGED SOFTWARE HAVE BEEN INSTRUMENTAL IN INTEGRATING THE COMPUTER INTO EVERYDAY LIFE. THESE SAME ADVANCES, HOWEVER, HAVE ALSO INCREASED SUBSTANTIALLY THE THREAT OF COMPUTER-RELATED CRIMES.

THE FBI HAS FOUND THAT COMPUTER CRIME IS OFTEN ONE OF THE MOST ELUSIVE CRIMES TO INVESTIGATE. IT MAY BE INVISIBLE. IT HAS NO GEOGRAPHIC LIMITATION, AND THE ENTIRE TRANSACTION MAY LAST LESS THAN A SECOND. IT CAN ALSO THREATEN THE INTEGRITY AND RELIABILITY OF SENSITIVE

COMPUTER SYSTEMS. DESPITE A GROWING INTEREST IN THE PROBLEM, A CONSISTENTLY APPLIED AND UNIVERSALLY ACCEPTED DEFINITION OF COMPUTER CRIME HAS NOT YET BEEN AGREED UPON BY THOSE CONCERNED WITH LAW ENFORCEMENT IN THIS AREA. THE FBI HAS FOUND THAT MANY COMPUTER CRIMES ARE MUCH LIKE TRADITIONAL CRIMES; THE CRIMINAL USES A COMPUTER AS THE INSTRUMENT OF THE OFFENSE INSTEAD OF THE FORGER'S PEN AND FRAUDULENT DOCUMENTS. OTHER ACTIVITIES, HOWEVER--SUCH AS UNLEASHING DESTRUCTIVE VIRUSES--ARE UNIQUE TO COMPUTERS. ALL HAVE THE POTENTIAL FOR CAUSING GREAT FINANCIAL LOSS OR DENIAL OF SERVICE IN A MATTER OF SECONDS OR FOR CAUSING DESTRUCTIVE EFFECTS THAT CAN LAST FOR DAYS, WEEKS OR MONTHS.

IN 1982 AND 1983, THE FBI VOICED CONCERN ABOUT PROBLEMS IN THE APPLICATION OF TRADITIONAL CRIMINAL STATUTES TO COMPUTER TECHNOLOGY. IN OCTOBER 1984, THE COMPUTER FRAUD AND ABUSE ACT WAS SIGNED INTO LAW. ONE ASPECT OF THAT ACT CRIMINALIZED UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS, COMMONLY REFERRED TO AS "HACKING." IN 1986, THIS LAW WAS AMENDED AND EXPANDED IN SCOPE TO INCLUDE "FEDERAL INTEREST COMPUTERS." THESE ARE DEFINED AS COMPUTERS USED EXCLUSIVELY BY FINANCIAL

INSTITUTIONS OR THE UNITED STATES GOVERNMENT, OR COMPUTERS THAT ARE ONE OF TWO OR MORE COMPUTERS LOCATED IN DIFFERENT STATES AND USED IN COMMITTING AN UNDERLYING OFFENSE. THE ACT PROVIDES CRIMINAL SANCTIONS FOR CERTAIN PROSCRIBED ACTS, FOR INTENTIONALLY ACCESSING A COMPUTER WITHOUT AUTHORIZATION, AND FOR EXCEEDING AUTHORIZED ACCESS. THE PROSCRIBED ACTS ARE THOSE INVOLVING TAKING, ALTERING, DAMAGING, OR DESTROYING INFORMATION AFFECTING THE OPERATION OF THE COMPUTER BY THE UNITED STATES GOVERNMENT, OR COMMITTING FRAUD AND OBTAINING ANYTHING OF VALUE.

THE COMPUTER FRAUD AND ABUSE ACT ALSO PROVIDED ANOTHER COMPUTER-ORIENTED CRIMINAL STATUTE TO PROSECUTE THIS TYPE OF CRIME. THE COMPANION STATUTE ADDRESSES FRAUD AND RELATED ACTIVITY IN CONNECTION WITH ACCESS DEVICES. PRIOR TO THE PASSAGE OF THESE LAWS, COMPUTER-RELATED CRIMES, AND, FOR THAT MATTER, THE VAST MAJORITY OF CASES MEETING FEDERAL PROSECUTIVE GUIDELINES HAVE BEEN PROSECUTED UNDER THE FRAUD BY WIRE STATUTE. IN ADDITION, OTHER STATUTES HAVE BEEN PASSED RECENTLY THAT ADDRESS THE ISSUE OF COMPUTER-RELATED CRIME. THESE CONCERN MALICIOUS MISCHIEF RELATING TO COMMUNICATIONS LINES, STATIONS OR SYSTEMS, AND

INTERFERENCE WITH THE OPERATION OF A SATELLITE. OTHER STATUTES ADDRESS THE MANUFACTURE, DISTRIBUTION, POSSESSION, AND ADVERTISING OF WIRE, ORAL, OR ELECTRONIC COMMUNICATION INTERCEPTING DEVICES AND PROHIBITED AND UNLAWFUL ACCESS TO STORED COMMUNICATIONS. ALL OF THESE FEDERAL VIOLATIONS ARE WITHIN THE PRIMARY JURISDICTION OF THE FBI, AND ALL RECOGNIZE VARIOUS ASPECTS OF ELECTRONIC AND COMPUTER CRIMINALITY.

IN THE CONTEXT OF OUR INVESTIGATIVE RESPONSIBILITIES, WE HAVE FOUND THAT EXISTING FEDERAL STATUTES ARE GENERALLY ADEQUATE WHEN THE COMPUTER-RELATED CRIMINAL ACTS PARALLEL COMMON LAW CRIMES SUCH AS EMBEZZLEMENT, FRAUD, THEFT, AND DESTRUCTION OF PROPERTY. WHILE COMMON LAW CONCEPTS OF THEFT INVOLVE A TAKING AWAY OF PROPERTY, HOWEVER, IT SHOULD BE NOTED THAT WITH COMPUTERS, INFORMATION CAN BE STOLEN WITHOUT THE OWNER OF THAT INFORMATION BEING AWARE OF THE THEFT OR WITHOUT INTERFERING WITH HIS ABILITY TO USE THE INFORMATION. RECENT LEGISLATION CRIMINALIZING UNAUTHORIZED ACCESS IN CONJUNCTION WITH ONE OF THESE OFFENSES HAS ALSO BEEN EFFECTIVE. EXISTING CRIMINAL STATUES, HOWEVER, ARE NOT SPECIFIC ON THE QUESTION OF WHETHER UNAUTHORIZED ACCESS IS A CRIME

WHERE NO THEFT OR DAMAGE OCCURS, AND THERE IS NO STATUTE SPECIFICALLY ADDRESSING VIRUSES. CURRENT CRIMINAL STATUTES, BY AND LARGE, ADDRESS THE ISSUE OF COMPUTERS AS THE VEHICLE OF THE CRIME. AS MORE SENSITIVE INFORMATION BECOMES STORED IN COMPUTERS AND AS GOVERNMENT AND INDUSTRY BECOME MORE DEPENDENT UPON THE PROPER FUNCTIONING OF COMPUTERS, WE HAVE SEEN AN INCREASE IN CRIMES IN WHICH THE COMPUTER OR COMPUTERIZED INFORMATION IS THE TARGET OF THE CRIME. COMPUTER VIRUSES PRESENT ONE SUCH EXAMPLE.

ON THE SUBJECT OF VIRUSES, THE FBI REGARDS A COMPUTER VIRUS AS ANY COMPUTER PROGRAM NOT READILY DISCERNIBLE TO THE USER THAT HAS THE CAPACITY TO INFECT OTHER COMPUTER SYSTEMS BY RECREATING ITSELF RANDOMLY OR CAUSING SOME OTHER SPECIFIC ACTION IN SOME PRE-DETERMINED CIRCUMSTANCE. A VIRUS IS USUALLY PLACED IN A SYSTEM BY A PERSON WHO HAS AUTHORIZED ACCESS, BUT IT CAN BE PLACED BY A "HACKER." IT MAY OR MAY NOT CAUSE DAMAGE, DESTRUCTION, OR UNAUTHORIZED ACCESS. COMPUTER VIRUSES DIFFER IN EFFECT DEPENDING ON THE INTENT, AND SOMETIMES THE COMPETENCE, OF THE DESIGNER. THE EFFECT CAN RANGE FROM BEING NEARLY HARMLESS TO BEING DEVASTATING, CAUSING COMPLETE

SHUTDOWNS OF SYSTEMS AND THE MASSIVE DESTRUCTION OF DATA. CLEANING UP THE AFTERMATH COULD COST MORE THAN THE DAMAGE TO THE SYSTEM. VIRUSES CAN BE TRANSMITTED BY INFECTED SOFTWARE, THROUGH NETWORKS, OR FROM REMOTE LOCATIONS. WITH TODAY'S TECHNOLOGY, VIRUSES CAN BEGIN THE INFECTIOUS PROCESS FROM A HOME PERSONAL COMPUTER, AN OFFICE, AN ACADEMIC INSTITUTION, OR FROM ALMOST ANYWHERE IN THE WORLD.

EXPERTS IN THIS FIELD HAVE FOUND THAT THE MOTIVES FOR CREATION OF VIRUSES INCLUDE INTELLECTUAL CURIOSITY, DESIRE FOR PUBLICITY OR NOTORIETY, DELIBERATE DENIAL OF SERVICE AND INDUSTRIAL OR OTHER SABOTAGE OF COMPUTER SYSTEMS AND DATA BANKS. VIRUS CREATORS RANGE FROM YOUNG STUDENTS WHO FAIL TO ANTICIPATE THE CONSEQUENCE OF CREATING AND TRANSMITTING A VIRUS TO DISGRUNTLED EMPLOYEES AND OTHERS WHO CLEARLY INTEND A MALICIOUS ACT. VIRUSES ARE EASY TO CREATE AND PROPAGATE, REQUIRE LITTLE EXPERTISE, AND MAY BE NEARLY IMPOSSIBLE TO PREVENT OR DETECT.

VIRUSES ARE OFTEN DIFFICULT TO TRACE AND ARE FREQUENTLY NOT DISCOVERED UNTIL IT IS TOO LATE TO PREVENT THE INTENDED HARM. INVESTIGATION MAY BE

COMPLICATED BY THE MANY PERMUTATIONS VIRUSES CAN UNDERGO AND BY THE WIDESPREAD GEOGRAPHIC AREAS INVOLVED. VIRUSES ARE FREQUENTLY DESIGNED TO PREVENT DETECTION. IN ADDITION, SOMETIMES THE OWNERS OF THE SYSTEMS ARE MORE CONCERNED WITH REPAIRING THE DAMAGE THAN WITH PROSECUTION OF THE OFFENDER. BECAUSE A VIRUS MAY CAUSE ONLY A SMALL AMOUNT OF DAMAGE TO MANY DIFFERENT USERS, NO SINGLE USER MAY CONSIDER THE EVENT SIGNIFICANT ENOUGH TO REPORT IT.

THE FBI'S INVESTIGATIONS OF COMPUTER-RELATED CRIMES GENERALLY HAVE BEEN SUCCESSFUL, BUT OUR INVESTIGATIVE EXPERIENCE WITH COMPUTER VIRUSES HAS BEEN LIMITED. QUITE FRANKLY, THE FBI HAS ONLY CONDUCTED CRIMINAL INVESTIGATIONS OF VIRUSES ON TWO OCCASIONS. ONE EXAMPLE OF A RECENT SUCCESS IS THE FBI INVESTIGATION OF A YOUNG COMPUTER HACKER WHO WENT BY THE ALIAS "SHADOW HAWK." THIS 18-YEAR-OLD SUCCESSFULLY ENTERED COMPUTERS OWNED AND OPERATED BY AT&T AND THE UNITED STATES GOVERNMENT. HE WAS ABLE TO COPY OVER A MILLION DOLLARS IN PROPRIETARY SOFTWARE, CAUSING SUBSTANTIAL DAMAGE IN THE PROCESS. HE WAS PROSECUTED UNDER THE CRIMINAL

STATUTE I JUST MENTIONED (THE COMPUTER FRAUD AND ABUSE ACT) AND SENTENCED IN FEBRUARY OF THIS YEAR.

I WOULD LIKE TO DISCUSS BRIEFLY OUR EFFORTS TO ENSURE THAT THE FBI HAS THE NECESSARY EXPERTISE TO ADDRESS COMPUTER CRIME EFFECTIVELY. THE DEVELOPMENT BY OUR INVESTIGATORS OF EXTREMELY SPECIALIZED EXPERTISE IN COMPUTER TECHNOLOGY IS IN FACT NOT OUR GOAL. WE ALREADY HAVE PERSONNEL WITH ADVANCED DEGREES IN ENGINEERING AND COMPUTER SCIENCES WHO CLEARLY HAVE THE NECESSARY EXPERTISE AND CAPABILITY. WE HAVE HUNDREDS OF COMPUTER LITERATE INVESTIGATORS AND THE TECHNICAL PERSONNEL TO ASSIST THEM. WE UTILIZE BOTH INTERNAL AND EXTERNAL TRAINING AND HAVE ACCESS TO THE MOST ADVANCED EXPERTISE IN OTHER GOVERNMENT AGENCIES, PRIVATE SECTOR COMPUTER FIRMS, AND EDUCATIONAL INSTITUTIONS. OUR STRATEGY IS TO EMPLOY A TEAM APPROACH TO VIRUS AND OTHER COMPUTER CRIME INVESTIGATIONS, UTILIZING INDIVIDUALS FROM VARIOUS DISCIPLINES. WE BELIEVE AN INVESTIGATIVE TEAM TAILORED TO THE THREAT BEING ADDRESSED IS THE BEST APPROACH. THE PROBLEMS I FORESEE FOR THE FBI RELATE NOT TO THE LEVEL OF EXPERTISE BUT TO THE NUMBER OF EXPERTS AND THE RESOURCES WE WILL HAVE TO

DEPLOY IF THIS POTENTIALLY EXPLOSIVE NEW AREA OF COMPUTER ACTIVITY CONTINUES TO EXPAND.

THE FBI HAS DEVELOPED UNIQUE AND SPECIALIZED TRAINING FOR ITS AGENTS AND OTHER LAW ENFORCEMENT PERSONNEL. SINCE 1976, THE FBI HAS OFFERED SPECIALIZED TRAINING FOR INVESTIGATORS OF COMPUTER-RELATED CRIMES AT OUR ACADEMY IN QUANTICO, VIRGINIA. WE EMPLOY THREE LEVELS OF TRAINING FOR COMPUTER CRIME INVESTIGATORS: 1) AN AWARENESS LEVEL, 2) A COMPREHENSIVE LEVEL, AND, 3) A SPECIALIST LEVEL. TO DATE, APPROXIMATELY 520 FBI SPECIAL AGENTS, AS WELL AS NUMEROUS LOCAL AND FOREIGN LAW ENFORCEMENT OFFICERS, HAVE GRADUATED FROM AN INTENSIVE THREE-WEEK COURSE. WE HAVE TRAINED OVER 250 INVESTIGATORS FROM OTHER AGENCIES IN ONE WEEK SCHOOLS AND HAVE TAKEN OUR INSTRUCTION INTO LOCAL COMMUNITIES, WHERE WE HAVE DELIVERED TRAINING TO OVER 1,400 STATE AND LOCAL LAW ENFORCEMENT OFFICERS. IN ONLY THE LAST THREE FISCAL YEARS, 220 SPECIAL AGENTS AND OVER 600 LOCAL OFFICERS HAVE RECEIVED THIS TRAINING. THESE COMPUTER-RELATED SCHOOLS ARE PROVIDING THE SKILLS THAT OUR AGENTS AND OTHER LAW ENFORCEMENT OFFICERS NEED IN THIS HIGHLY TECHNICAL ARENA.

IN ADDITION, PERSONNEL AT QUANTICO ARE IN THE FOREFRONT OF RESEARCH EFFORTS ON COMPUTER SECURITY, THE NATURE AND IMPACT OF VIRUSES, AND RELATED MATTERS. WE ARE EVEN DEVELOPING BEHAVIOR PROFILES OF COMPUTER "HACKERS."

LAW ENFORCEMENT ASIDE, THE SECURITY OF COMPUTER SYSTEMS RESTS WITH THE DESIGNERS OF HARDWARE, THE COMPOSERS OF SOFTWARE AND THE OWNERS OF COMPUTERS. VERIFYING THE AUTHENTICITY OF THE SOFTWARE BEING USED TO REDUCE VULNERABILITY TO COMPUTER VIRUSES IS ONE MAJOR STEP THAT CAN CONTRIBUTE TO COMPUTER SECURITY. SUCCESSFUL PROSECUTIONS WILL ALSO HAVE A DETERRENT EFFECT. BUT ULTIMATELY, ENHANCEMENTS TO SECURITY WILL BE REQUIRED TO CURB THE SPIRALING INCREASE IN COMPUTER CRIME.

THERE MUST ALSO BE A BALANCE BETWEEN THE BENEFITS DERIVED FROM EDUCATIONAL EXPERIMENTATION AND THE FREE FLOW OF INFORMATION, ON THE ONE HAND, AND THE NEED TO PREVENT CRIMINAL ACTIVITY HAVING THE POTENTIAL FOR MILLIONS OF DOLLARS IN DAMAGE ON THE OTHER. ONCE THE BALANCE TIPS TO CRIMINAL ACTIVITY, THE FBI INTENDS TO PURSUE VIGOROUSLY

THOSE WHO VIOLATE FEDERAL LAW THROUGH THE CREATION AND INTRODUCTION OF VIRUSES.

MR. CHAIRMAN, THAT CONCLUDES MY FORMAL REMARKS.

The Subcommittee on Technology and the Law
of the Senate Judiciary Committee

Written Statement of Clifford Stoll
Harvard - Smithsonian
Center for Astrophysics
Cambridge, MA 02138
617/495-7147

The twenty scientists using my computer share common interests -- we're trying to solve fundamental questions of the universe. Elsewhere in my building, are other computers, for secretaries, scientists, and technicians. All of us are linked together through a local network.

This network lets us share data, programs, news, and gossip. A student on another floor writes a paper using data that I send to her. She, in turn, mails progress reports to our department head. We post announcements of meetings and parties over our network.

Our local computer network forms a neighborhood of people working together.

We talk with the outside world through a dozen other networks. The Internet, once called the Arpanet, lets us talk to researchers across the country. Thanks to this system, it takes a minute to send a message from Los Angeles to New York. From my desk, I can run programs in Berkeley, Boston, or Bangor. By communicating over the computer networks, we collaborate in projects which are impossible in isolation.

These wide area networks are communities -- no less real than those in the rest of society.

Our cities and towns are tied together by streets, roads, state highways, and the interstates. Similarly, our communities of computers are linked through local, regional, and national networks. Our highways transport food and equipment; our networks transport ideas. The Internet is probably the most important thoroughfare created over the past twenty years.

The networks and highways have the same headaches: too much traffic, expensive maintenance, and figuring out who will pay for them.

Unknown to this penetrator, while he was breaking into computers, we were monitoring him and tracing his connections. At first, it was difficult to get the attention of federal law enforcement agencies -- not many front line investigators have technical training. Later, with the help of the FBI's Alexandria Virginia Field Office, and the Air Force Office of Special Investigations, we ultimately traced the intruder back to Hannover, West Germany.

To track down this person, we planted bogus information about a fictitious SDI network in our computer. He swallowed the bait -- copying those files into his Hannover computer. Our trace complete, we thought our job was done. But three months later, we received a letter from someone in Pittsburgh, PA, asking for more information about our SDI networks.

From this, we determined that someone in Hannover was systematically collecting sensitive information, and selling it for cocaine and money to Soviet Bloc agents. They, in turn, likely hired a representative in Pittsburgh to validate the data and to extract additional information.

Catching this spy took a year of full time effort. While he was reaching into our computers, I lost a year of astronomy research. Worse -- much worse -- a thief was stealing information from our nation's computers.

This woke me up. Our networks -- the very lifeblood of our computer community -- were being exploited for espionage. That this attempt failed was only a fortuitous accident. I wonder how many times others have succeeded.

Computer Viruses

Computer viruses are sections of code which duplicate themselves into ordinary programs. Usually, they propagate by infecting programs run on personal computers. Once a program is infected, it will infect any computer that runs that program. Viruses spread by interchanging programs, either by floppy disk or by copying to electronic bulletin boards.

Some viruses are benign. They merely spread themselves without interfering with the program's normal operation. More often, though, viruses have malicious side effects -- erasing your files or corrupting your data.

The job wasn't made any easier by the writer of the virus. The program was purposely hidden, written to obscure itself and its mechanisms. The writer exploited not one, but several weaknesses in the Unix software, making it difficult to understand and tough to control.

As one of the early discoverers of the virus, I contacted appropriate authorities. At 4 AM EST, I called the Network Operations Center and described the problem; at 6:30AM, I called the National Computer Security Center, and numerous systems managers around the country.

The antidotes and patches to counteract the virus were developed entirely at academic institutes, especially the University of California at Berkeley and MIT. No governmental organization unwound the virus or published patches. Academics responded immediately -- and voluntarily -- to this national need.

How much damage was done? Early on, about 6000 computers were estimated to be infected. Based on my own survey, between 2000 and 3000 computers were hit by the Internet worm. Published estimates of $90 million in damages are grossly overblown and self-serving; I estimate the loss at less than one million dollars -- still, a significant loss.

Conclusion

How do I view these incidents? As a harmless prank? As a cute college trick to razz programmers?

Hardly. If someone disabled several thousand cars for an afternoon, would it be considered a harmless prank? Yet my computer costs the same as a car, and it's essential for my job. For two days, I couldn't work.

Or might this virus be a useful way to raise our consciousness of computer security? A quaint attempt to tell us to secure our computers?

We don't thank burglars for reminding us that our houses are insecure. Nor do we thank someone for teaching us that our computers can be wrecked. There are more ethical ways to spread the word.

Yet how should we react? One response is to slam doors, and build barriers against outsiders. This will make it tougher for the virus-writers. It'll also make life difficult for those who need to exchange information.